UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

OUSSAMA EL OMARI, Plaintiff, v. DECHERT LLP, NICHOLAS PAUL DEL ROSSO, and VITAL MANAGEMENT SERVICES, INC., Defendants.	Civil Action No. 23-cv-04607 (LAK) (OTW) **ORAL ARGUMENT REQUESTED**

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT DECHERT LLP'S MOTION TO DISMISS

Sean Hecker
John C. Quinn
David Gopstein
Mark Weiner
KAPLAN HECKER & FINK LLP
350 Fifth Avenue, 63rd Floor
New York, NY 10118
Tel: (212) 763-0883
Fax: (212) 564-0883
shecker@kaplanhecker.com
jquinn@kaplanhecker.com
dgopstein@kaplanhecker.com
mweiner@kaplanhecker.com

Carmen Iguina González*
KAPLAN HECKER & FINK LLP
1050 K Street NW, Suite 1040
Washington, DC 20001
Tel: (212) 763-0883
Fax: (212) 564-0883
ciguinagonzalez@kaplanhecker.com

**Pro hac vice application forthcoming*

Attorneys for Defendant Dechert LLP

August 25, 2023

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

Defendant Dechert LLP ("Dechert") respectfully submits this memorandum of law in support of its motion to dismiss Plaintiff's Complaint filed on June 1, 2023.

PRELIMINARY STATEMENT

Plaintiff Oussama El Omari ("Omari") continues his march towards serial litigator status with this, his fourth litigation in seven years (and second against Dechert), all arising from his former employ with an instrumentality of Ras al Khaimah ("RAK"), one of the seven emirates of the United Arab Kingdom. The three prior litigations were dismissed at the pleading stage in decisions that were upheld on appeal. This new case should meet the same fate.

In this iteration, Omari alleges that his emails were hacked so that they could be used in the prior litigations by Dechert, who acted as counsel for the defendants (and itself) in two of those prior cases. More specifically, Omari contends that an Indian hacking firm illegally accessed his email accounts at the direction of Defendants Nicholas Del Rosso and Vital Management Services, who had been engaged as contractors by Dechert in its representations of RAK dating back to 2014. Nowhere in this Complaint does Omari allege that Dechert directed or otherwise contributed to the hacking; indeed, he does not even allege that Dechert was ever provided the purportedly hacked emails. Yet he still accuses Dechert of violating, and conspiring to violate, the Computer Fraud and Abuse Act ("CFAA" or "the Act") and North Carolina state law through this alleged unauthorized access.

As set forth herein, even assuming the truth of the allegations contained in the Complaint, Omari's claims are insufficient as a matter of law. *First*, the CFAA claims fails because the "loss" Omari maintains he suffered is not actionable under the statute, as the Supreme Court has recently affirmed. *See Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021). The CFAA claim against Dechert also fails because the Complaint nowhere alleges that Dechert was involved in the

hacking. *Second*, the Complaint's attempt to entangle Dechert in an alleged conspiracy to violate the CFAA fails too—not only because the Complaint fails to allege a substantive violation of the Act by the conspirators, but also because it does not allege any facts that could lead to a reasonable inference that Dechert entered into an agreement to hack Plaintiff's emails. And *third*, the Complaint's state-law claim fails because it is well beyond the applicable statute of limitations. Although Plaintiff insists that he did not learn of the unauthorized access until this year, accrual of the North Carolina conversion claim depends solely on the date of the alleged conversion, and per Plaintiff's own allegations, that occurred in 2017, well outside the three-year statute of limitations period. For these and other reasons set forth below, this complaint, like his last three, should be dismissed.

PLAINTIFF'S ALLEGATIONS[1]

As noted above, this is the fourth litigation Plaintiff has filed in seven years stemming from his former role as Director and CEO of the RAK Free Trade Zone Authority ("RAKFTZA"), an instrumentality of RAK. *See* ECF No. 1 ("Complaint") ¶¶ 17–18 (describing two of the prior litigations). Two of the earlier litigations involved Dechert. In the first, Plaintiff brought claims in this District against RAKFTZA and related groups based on the alleged preparation of a "false smear report" that served as the pretext for his termination from his position at RAKFTZA. *Id.* ¶ 17. Dechert, through its former partner Linda Goldstein, represented RAKFTZA in that litigation. *Id.* ¶ 17. Four years later, Plaintiff alleged that Dechert, former Dechert partner Neil Gerrard, and others had conspired to organize a "false smear campaign" against him. *Id.* ¶ 18.

[1] On this motion, the well-pleaded allegations of the Complaint are assumed to be true. *McCarthy v. Dun & Bradstreet Corp.*, 482 F.3d 184, 191 (2d Cir. 2007); *see also Dane v. UnitedHealthcare Ins.*, 974 F.3d 183, 188 (2d Cir. 2020). Dechert reserves all rights to—and does—dispute many of the allegations summarized herein. Moreover, Defendants and the Court are "not required to credit conclusory allegations or legal conclusions couched as factual . . . allegations." *Id.*

Dechert, again through Goldstein, represented itself and Gerrard in this latter litigation. *Id.* Both prior litigations were dismissed at the pleading stage, and both dismissals were upheld on appeal. *Id.* ¶¶ 17–18.[2] Notably, in those prior litigations, Plaintiff also brought—and this Court rejected—claims under the CFAA. *See El Omari v. Buchanan*, No. 20 CIV. 2601 (VM), 2021 WL 5889341, at *13 (S.D.N.Y. Dec. 10, 2021), *aff'd*, No. 22-55-CV, 2022 WL 4454536 (2d Cir. Sept. 26, 2022); *Omari v. Ras Al Khaimah Free Trade Zone Auth.*, No. 16 CIV. 3895 (NRB), 2017 WL 3896399, at *11 (S.D.N.Y. Aug. 18, 2017), *aff'd sub nom. El Omari v. Kreab (USA) Inc.*, 735 F. App'x 30 (2d Cir. 2018). Plaintiff refers to these two litigations together throughout his Complaint as the "NY Litigation." *See, e.g.*, Compl. ¶ 13. Plaintiff was represented in those litigations by his attorney in the present litigation. *Id.* ¶ 16.

I. The U.K. Litigation and Devices at Issue

According to Plaintiff's allegations here, his email account was hacked on or about January 12, 2017 at the direction of a private investigator, Defendant Nicholas Del Rosso, and his company, Defendant Vital Management Services ("VMS"), that Dechert had previously engaged on its client's behalf. *Id.* ¶¶ 1, 20, 22. Plaintiff says he learned of this hacking in January 2023 when he received a "foreign notice pursuant to a U.K. court order." *Id.* ¶ 19. That notice informed him of the existence of three devices that are at issue in ongoing litigation in the U.K.[3] *Id.* One

[2] Plaintiff filed a third litigation in 2019 against the International Criminal Police Organization ("Interpol"), alleging that Interpol violated his rights as a result of his being scapegoated in a political conflict in RAK. *See Omari v. Int'l Crim. Police Org. – Interpol*, No. 19 CIV. 1457, ECF No. 1, ¶ 52 (E.D.N.Y. Mar. 13, 2019). That, too, was dismissed. *Omari v. Int'l Crim. Police Org. - Interpol*, No. 19 CIV. 1457 (SJ) (PK), 2021 WL 1924183, at *7 (E.D.N.Y. May 13, 2021), *aff'd*, 35 F.4th 83 (2d Cir. 2022), *cert. denied*, 143 S. Ct. 214 (2022).

[3] The U.K. proceedings in which the Laptop is at issue comprise (1) *Al Sadeq v. Dechert & Others*, Claim No. QB-2020-000322 ("Al Sadeq Proceedings"); (2) *Quzmar v. Dechert & Another*, QB-2020-003142 ("Quzmar Proceedings"); (3) *Stokoe Partnership v. Dechert & Another*, Claim No. QB-2020-002492 ("Stokoe Proceedings"); (4) *Mikadze & Massaad v. Dechert & Others*, Claim

of those devices, a Huawei Matebook laptop ("the Laptop"), allegedly contains "a backup copy of emails containing the email address of El Omari's undersigned counsel (smm@milopc.com)." *Id.* ¶¶ 19–20. The emails allegedly include "communications between El Omari and his undersigned attorney," and their date range is said to encompass the period of the NY Litigation. *Id.* Neither of the other two devices is alleged to contain Plaintiff's emails.

In the U.K. litigation, Defendant Del Rosso asserted a claim of ownership over the Laptop, which as of the time of the Complaint was in the possession of Stokoe Partnership Solicitors ("Stokoe"), counsel for the plaintiffs in that litigation. *Id.* The U.K. Court has actively addressed that claim and found in Defendant Del Rosso's favor. *See* Declaration of John C. Quinn ("Quinn Decl."), Ex. 1 (*Del Rosso v. Stokoe Partnership Solicitors, Al Sadeq v. Dechert LLP, Quzmar v. Dechert LLP, Stokoe Partnership Solicitors v. Dechert LLP, Mikadze v. Dechert LLP*, [2023] EWHC 2112 (KB)) ¶ 1. Indeed, following a July 31, 2023 hearing, the U.K. Court ordered Stokoe to deliver the Laptop to English counsel for Defendants Del Rosso and VMS, who is directed to engage an independent forensic IT specialist to conduct searches of the information contained on the device. *See id.*[4]

No. KB-2023-001629 ("Mikadze/Massaad Proceedings"); (5) *Ras al Khaimah Investment Authority v. Azima v. Dechert & Others*, Claim No. HC-2016-002798 ("Azima Proceedings"); (6) *Buchanan v. Stokoe*, Claim No. KB-2023-001629 ("Buchanan Proceedings"); and (7) *Del Rosso & Vital Management v. Stokoe*, Claim No. KB-2023-002877 ("Del Rosso Proceedings") (collectively, "the U.K. litigation"). Some of the U.K. litigation was commenced after the notice received by Plaintiff.

[4] The Court may take judicial notice of the "status of other lawsuits in other courts and the substance of papers filed in those actions" and thus may consider the status of and filings in the related litigations referenced herein. *Schenk v. Citibank/Citigroup/Citicorp*, No. 10 CIV. 5056 (SAS), 2010 WL 5094360, at *2 (S.D.N.Y. Dec. 9, 2010); *see also Anderson v. Rochester–Genesee Reg'l Transp. Auth.*, 337 F.3d 201, 205 (2d Cir. 2003) (taking judicial notice of district court opinion not in appellate record); *Rothman v. Gregor*, 220 F.3d 81, 92–93 (2d Cir. 2000) (taking judicial notice of complaint in another action). Judicial notice is appropriate "not for the

II. Plaintiff's Investigation Into the Alleged Hacking

After receiving the "foreign notice," Plaintiff performed an investigation into the purported hacking. Compl. ¶¶ 22–31. The investigation allegedly revealed that one of Plaintiff's email accounts—ceo@oussamaeelomari.com—was hacked "on or about January 12, 2017." *Id.* ¶ 22. Plaintiff infers that the email tranche found on the Laptop was copied from this account. *Id.* The investigation indicated that the hacking resulted from three phishing emails Plaintiff received in December 2016 and January 2017 to two of his email addresses. *Id.* ¶¶ 23, 31. Plaintiff opened and clicked on a link in a malicious attachment attached to a January 12, 2017 email, and that resulted in the acquisition by the hacker of the credentials for Plaintiff's ceo@oussamaeelomari.com account, from which the hacker purportedly copied Plaintiff's emails. *Id.* ¶ 27.

Based solely on the alleged existence of his attorney's emails on the Laptop belonging to Del Rosso, Plaintiff speculates that the emails were "use[d] against him in the NY litigation" by providing "intelligence about El Omari's knowledge and information about the Ruler, legal positions, strategies, witnesses, evidence, and funding." *Id.* ¶¶ 13, 30. Plaintiff does not allege the contents of any of the emails; how that content could have "assisted" Dechert in defending his claims (which, again, were dismissed at the pleading stage); nor even that the emails or their contents were ever provided to Dechert.

III. The Alleged Conspiracy

Plaintiff alleges that the hacking was performed by hackers from CyberRoot Risk Advisory Private Limited ("CyberRoot"), an Indian firm, and that CyberRoot was paid to obtain Plaintiff's

---

truth of the matters asserted in the other litigation, but rather to establish the fact of such litigation and related filings." *Kramer v. Time Warner Inc.*, 937 F.2d 767, 774 (2d Cir. 1991).

emails by Defendant Del Rosso. *Id.* ¶¶ 7, 32. Del Rosso—via VMS's bank in North Carolina—purportedly sent "dozens of international wire transfers" totaling more than $500,000 to CyberRoot's Indian bank between July 2015—a year and a half before the alleged hacking—and December 2016. *Id.* ¶¶ 33–34.

Apparently based on these payments to CyberRoot and Del Rosso's engagements by Dechert, Plaintiff alleges that Dechert, Del Rosso, and VMS conspired with others, including CyberRoot, "to hack and access confidential emails of El Omari, and other Dechert LLP's litigation adversaries." *Id.* ¶ 36. Del Rosso, Plaintiff alleges, had "actual knowledge of the illegal activities." *Id.* ¶ 37. Plaintiff again speculates that Dechert "either had actual knowledge, or must have strongly suspected the illegal hacking activities of its private investigator Del Rosso and CyberRoot." *Id.* ¶ 38. That is purportedly because the money paid by Del Rosso to CyberRoot was "in turn costs to Dechert," and the information allegedly revealed in the confidential emails "must have triggered strong suspicions by Goldstein," Dechert's former partner and counsel in Plaintiff's previously dismissed cases. *Id.* ¶ 38. Goldstein, Plaintiff alleges, "must have deliberately avoided learning about the illegal sourcing of the sensitive information." *Id.* Plaintiff never alleges, however, that Goldstein entered into any agreement with Del Rosso or others regarding the hacking, or that she, or anyone at Dechert, directed, encouraged, or paid for it. *Id.* Nor does he allege that the emails were provided to Goldstein or anyone else at Dechert. *Id.*

IV. Plaintiff's Claims

As a result of the unauthorized access of his emails, Plaintiff allegedly suffered "injuries to his business and property." *Id.* ¶ 42. He asserts that his damages "are in excess of tens of thousands of dollars paid to date in legal fees and costs, and forensic computer investigation costs

related to investigating, assessing the scope of the hacking, and seeking to remedy the complete loss of the confidentiality of the emails." *Id.* ¶ 41.

On the basis of the foregoing, Plaintiff alleges that Defendants violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C) (Count I); conspired to commit the same, in violation of 18 U.S.C. § 1030(b) (Count II); and committed conversion under the common law of North Carolina (Count III). Compl. ¶¶ 47–75.

STANDARD OF REVIEW

Federal Rule of Civil Procedure 12(b)(6) requires that a complaint "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A court first reviews plaintiff's complaint "to identify allegations that, 'because they are no more than conclusions are not entitled to the assumption of truth'"; it then considers whether the "remaining well-pleaded factual allegations . . . 'plausibly give rise to an entitlement to relief.'" *Reis, Inc. v. Lennar Corp.*, No. 15 CIV. 7905 (GBD), 2016 WL 3702736, at *3 (S.D.N.Y. July 5, 2016) (quoting *Iqbal*, 556 U.S. at 679).

ARGUMENT

Plaintiff brings two causes of action under the Computer Fraud and Abuse Act, and one under North Carolina common law. On all three, the Complaint fails to state a claim. *First*, the CFAA claims must be dismissed because Plaintiff fails to plead a cognizable "damage" or "loss" as required by the statute and binding precedent. Specifically, Plaintiff's claims for losses concerning attorneys' fees and costs and the loss of the confidentiality in his emails is not a cognizable "loss" under the CFAA. And although Plaintiff claims a loss relating to the forensic investigation he conducted following awareness of the hacking, the Complaint nowhere alleges

that the investigation sought to identify and remedy a *technological harm* caused by the hacking, nor does it specify the amount of loss attributable to that investigation, both of which are requirements under the CFAA. Moreover, Plaintiff fails to allege that Dechert itself played a role in violating the statute—a fatal flaw in his CFAA claim that Plaintiff has made in past unsuccessful attempts to litigate CFAA claims against other parties. *Second*, the CFAA conspiracy claim must be dismissed for the additional reason that the allegations of conspiracy are conclusory and insufficient to state a claim for relief that is plausible on its face. *Third*, the conversion claim must be dismissed because it is plainly barred by the governing statute of limitations.

I. The Complaint Fails to Plead a Claim Under the CFAA

The CFAA subjects to criminal liability one who "'intentionally accesses a computer without authorization or exceeds authorized access,' and thereby obtains computer information." *Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021) (quoting 18 U.S.C. § 1030(a)(2)). It also provides a private cause of action, pursuant to which persons suffering "damage" or "loss" from violations of the CFAA may sue for money damages and equitable relief. *See id.* (quoting 18 U.S.C. § 1030(g)). A civil action under the CFAA may proceed only if the plaintiff alleges certain kinds of "'damage or loss' of at least $5,000 attributable to an alleged violation of the CFAA." *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 439 (2d Cir. 2004) (citing 18 U.S.C. § 1030(g) and *id.* § 1030(e)(8)). As noted above, in his past litigations, Plaintiff has twice tried, and twice failed, to bring CFAA claims. His claims here fare no better.

The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). And it defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the

offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* at § 1030(e)(11). In reading those definitions, courts have interpreted both terms narrowly. Just two years ago, the Supreme Court clarified that the CFAA's "damage" and "loss" "focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data." *Van Buren*, 141 S. Ct. at 1660. Such an interpretation of the terms "damage" and "loss" "makes sense in a scheme 'aimed at preventing the typical consequences of hacking.'" *Id.* (quoting *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F.3d 756, 760 (6th Cir. 2020)). And indeed, "[b]oth before and after the Supreme Court's decision in *Van Buren*, 'courts in this District [have] interpreted the CFAA to require loss related to damage or impairment of the target computer itself.'" *Rekor Sys., Inc. v. Loughlin*, No. 19 CIV. 7767 (LJL), 2022 WL 789157, at *11 (S.D.N.Y. Mar. 14, 2022) (quoting *El Omari v. Buchanan*, 20 CIV. 2601 (VM), 2021 WL 5889341, at *14 (S.D.N.Y. Dec. 10, 2021)). Only damages or losses that fall within the CFAA's definition of those terms may count towards satisfying the $5,000 threshold. *See Dreni v. PrinterOn Am. Corp.*, 486 F. Supp. 3d 712, 736–37 (S.D.N.Y. 2020) (excising unrecoverable losses in assessing whether threshold met).

Plaintiff alleges three forms of loss here: (1) "legal fees and costs," Compl. ¶ 50; (2) "forensic computer investigation costs related to investigating, assessing the scope of the hacking, and seeking to restore the complete loss of the confidentiality of the emails," *id.*; and (3) "loss of the valuable confidentiality of the data in the attorney-client communication emails which relate to El Omari's NY litigation," *id.* ¶ 52. These losses, he claims, have caused him "damages within a 1-year period in excess of $5,000 expended in forensic computer investigation costs and attorney fees in this proceeding." *Id.* ¶ 54.

A. The Complaint Fails to Plead Actionable "Loss" under the CFAA

The first and third categories of "loss" that Plaintiff alleges—legal fees and "loss of valuable confidentiality"—unquestionably fall outside the realm of what is recoverable under the CFAA. Because CFAA losses are limited to "remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made," costs unrelated to or too far removed from the accessed computer may not be recovered. *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474–76 (S.D.N.Y. 2004), *aff'd*, 166 F. App'x 559 (2d Cir. 2006). Thus, "litigation-related expenses do not qualify as 'losses' under the CFAA." *Dreni*, 486 F. Supp. 3d at 736 (collecting cases); *see also Goodman v. Goodman*, No. 21 CIV. 10902 (GHW) (RWL), 2022 WL 17826390, at *9 (S.D.N.Y. Dec. 21, 2022), *report and recommendation adopted*, No. 21 CIV. 10902 (GHW), 2023 WL 1967577 (S.D.N.Y. Feb. 12, 2023) (collecting cases holding the same after *Van Buren*). Nor do non-economic losses like "loss of the confidentiality" of emails. Compl. ¶ 52; *see Jensen v. Cablevision Sys. Corp.*, No. 17 CIV. 00100 (ADS) (AKT), 2017 WL 4325829, at *13 (E.D.N.Y. Sept. 27, 2017) (finding "invasion of . . . privacy" not a cognizable loss under CFAA). Plaintiffs' first and third forms of loss are therefore easily disposed.

Plaintiff's second category of loss—the "forensic computer investigation costs related to investigating, assessing the scope of the hacking, and seeking to restore the complete loss of the confidentiality of the emails," Compl. ¶ 50—also fails to plead a cognizable "loss" under the CFAA, for two reasons. *First*, this second category of loss is also simply not of the kind that is recoverable under the CFAA. While "the costs of investigating security breaches constitute recoverable 'losses,'" *Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 387 (S.D.N.Y. 2010), that is so only when the investigation is performed "to identify, investigate, or

remedy any *covered damage*," *Better Holdco, Inc. v. Beeline Loans, Inc.*, No. 20 CIV. 8686 (JPC), 2021 WL 3173736, at *4 (S.D.N.Y. July 26, 2021) (emphasis added). And "covered damage," as the Supreme Court, the Second Circuit, and courts in this District have interpreted that term under CFAA, includes only technological harm. *Id.*; *see also Van Buren*, 141 S. Ct. at 1660. As a court in this District already explained in rejecting one of Plaintiff's prior attempts at a CFAA claim, "the focus is on the connection between the plaintiff's response and 'damage to or impairment of the protected computer.'" *Buchanan*, 2021 WL 5889341, at *14 (citing *Better Holdco, Inc.*, 2021 WL 3173736, at *3).

Here, Plaintiff alleges vaguely that he initiated "an investigation to determine what email account was hacked to obtain the stolen email tranche." Compl. ¶ 22. He does not allege that the investigation sought to identify or assess any technological harm to the computer or its information. Instead, Plaintiff alleges only that the investigation was aimed at "seeking to restore the complete loss of the confidentiality of the emails." *Id.* ¶ 50. But this Court has repeatedly held that investigation into the downloading and copying of emails is not a covered "loss" under the CFAA. *See Better Holdco, Inc.*, 2021 WL 3173736, at *4 (finding allegation that data was downloaded and copied did not plead technological harm, and investigation into extent of misappropriation of confidential information was not covered loss); *Reis*, 2016 WL 3702736, at *6 (where plaintiff alleged he "expend[ed] time, money, and resources . . . to conduct an investigation into the intrusion and a damages assessment," CFAA claim insufficient absent "allegations that the investigation was for the purpose of looking into any damage to data, programs, or server system"); *Fink v. Time Warner Cable*, 810 F. Supp. 2d 633, 641 (S.D.N.Y. 2011), *on reconsideration*, No. 08 CIV. 9628 (LTS) (KNF), 2011 WL 5121068 (S.D.N.Y. Oct. 28, 2011) (allegations of losses "relating to time and effort in assessing 'damage' to each computer"

failed because they did not allege loss relating to remedying damage or restoring data to its prior condition). Plaintiff's alleged investigation to "restore the complete loss of confidentiality of the emails," Compl. ¶ 50, similarly fails to state a claim for technological harm that falls within the narrow ambit of the CFAA. Simply put, despite having been warned by the court in his previously-dismissed Complaints that his CFAA claims would fail absent an allegation of "damage to or impairment of the protected computer," *Buchanan*, 2021 WL 5889341, at *14, Plaintiff once again falls short here.

Second, even if Plaintiff's second category of alleged forensic-investigation loss were cognizable, his Complaint nowhere breaks down which portion of his expenses are attributable to investigatory costs resulting from Defendants' alleged conduct, rather than the categorically non-actionable legal fees and costs. Instead, Plaintiff lumps them all together and alleges broadly that he sustained damages "in excess of $5,000 expended in forensic computer investigation costs and attorney fees in this proceeding." Compl. ¶¶ 54, 66. Courts have found that insufficiently specific loss allegations can be fatal to a CFAA claim where, for example, plaintiffs plead damages without identifying the quantity of those losses resulting directly from the defendants' unauthorized access, *Reis*, 2016 WL 3702736, at *7 ("Plaintiffs do not specify which portion of any investigatory expenses resulted from Defendants' conduct"), or do not quantify the CFAA-specific loss at all, *LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 514 (S.D.N.Y. 2015) ("The . . . CFAA-specific allegation does not quantify the loss it alleges and therefore also does not satisfy the $5,000 threshold requirement."). Because Plaintiff has not provided allegations sufficient to allow the Court to subtract out the unrecoverable attorney fees from his alleged loss and determine that the remaining losses exceed $5,000, he has not met the $5,000-loss jurisdictional threshold and has not stated a claim under the CFAA. *Dreni*, 486 F. Supp. 3d at 736–37.

B. The Complaint Fails to Plead Dechert's Involvement

Even if Plaintiff had alleged a category of "loss" that would qualify under the CFAA, his Complaint has not alleged that *Dechert* engaged in conduct that caused that loss. To state a claim under Section 1030(a)(2)(c) of the CFAA, Plaintiff must plead that Dechert "intentionally access[ed] a computer without authorization." *Id.* He does no such thing. While Plaintiff alleges that Dechert "either had actual knowledge, or must have strongly suspected the illegal hacking activities," Compl. ¶ 38, the Complaint nowhere asserts that Dechert accessed Plaintiff's computer, or even that Dechert directed Defendant Del Rosso to hire CyberRoot to do so. As courts in this District have recognized time and time again, CFAA claims cannot lie where "Plaintiff has provided no facts to establish that [Defendant] is affiliated with the hack[] of Plaintiffs' computers." *Broidy v. Glob. Risk Advisors LLC*, No. 19 CIV. 11861 (MKV), 2021 WL 1225949, at *9 (S.D.N.Y. Mar. 31, 2021); *see also JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 526 (S.D.N.Y. 2013) (dismissing CFAA claim at pleading stage where plaintiff asserted only "speculative" allegations that defendants had hacked server).

Plaintiff has committed this same pleading failure twice previously. In *RAKFTZA*, this Court rejected his CFAA claim because "plaintiff does not allege sufficient factual matter to permit a 'reasonable inference' that RAKFTZA—as opposed to someone else—was involved in the hacking of plaintiff's website." 2017 WL 3896399, at *11. And in *Buchanan*, this Court again dismissed Plaintiff's CFAA claim because "El Omari fails to plausibly allege that Defendants—as opposed to someone else—were responsible for any purported hacking of El Omari's computer or conspired with Alison for that purpose." *Buchanan*, 2021 WL 5889341, at *13. Plaintiff's third bite at the apple should meet the same fate.

II. The Complaint Fails to Plead a Claim for Conspiracy to Violate the CFAA

Because Plaintiff has failed to plead a substantive violation of the CFAA, he has also failed to plead a claim for conspiracy to violate that statute under 18 U.S.C. § 1030(b). *See Espire Ads LLC v. TAPP Influencers Corp.*, Nos. 21 CIV. 10623 (JGK), 21 CIV. 11068 (JGK), 2023 WL 1968025, at *15 (S.D.N.Y. Feb. 13, 2023) (holding CFAA conspiracy claim failed where plaintiffs did not allege loss above the jurisdictional threshold); *Reis, Inc.*, 2016 WL 3702736, at *7 (citing *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 836 (N.D. Cal. 2014), and *PNC Mortgage v. Superior Mortgage Corp.*, CIV. A. No. 09-5084, 2012 WL 627995, at *4 (E.D. Pa. Feb. 27, 2012)).

But even if Plaintiff had adequately pleaded a threshold violation of the CFAA, his conspiracy claim against Dechert would still fail. Conspiracy claims require "specific allegations of an agreement and common activities" among co-conspirators. *NetApp, Inc.*, 41 F. Supp. 3d at 835–36 (collecting cases). Plaintiff has alleged neither. Specifically, "to survive a motion to dismiss, plaintiff must allege with sufficient factual particularity that defendants reached some explicit or tacit understanding or agreement." *Id.* at 836 (cleaned up).

Plaintiff does not come close to that pleading requirement here. As noted above, the only allegations Plaintiff levies with regard to Dechert as it concerns the alleged hacking is that "Dechert LLP either had actual knowledge, or must have strongly suspected the illegal hacking activities of its private investigator Del Rosso and CyberRoot." Compl. ¶ 38. Plaintiff does not allege that Dechert directed Del Rosso to hire CyberRoot, or came to any agreement with Del Rosso to do so. Although Plaintiff alleges that the "sharing of the sensitive information gleaned from the stolen confidential emails with Goldstein at Dechert NY must have triggered strong suspicions by Goldstein, an experienced and learned law professional, that El Omari's sensitive

litigation information was illegally obtained," *id.*, the Complaint does not allege that Goldstein or Dechert were in fact provided with any of the supposedly hacked data or emails, let alone that they agreed with others to hack the data or otherwise access Plaintiff's emails in the first place. And although Plaintiff contends that Defendants Del Rosso and VMS paid CyberRoot over $500,000 from July 2015 to December 2016 and that these were "in turn costs to Dechert," the Complaint never alleges any facts to support Plaintiff's conjecture that the money was coming from Dechert, and even if it did, the Complaint does not allege that the supposed "costs" would have been identifiable as having anything to do with hacking. *Id.* In short, the Complaint fails to allege the requisite agreement.

Plaintiff instead asks this Court to presume an agreement between Defendant Dechert and Defendants Del Rosso and VMS based on conclusory and unsupported allegations of implicit knowledge and the supposed payment of costs (including supposed hacking fees) that the Complaint nowhere alleges Dechert actually paid. That is clearly insufficient. *See Dane*, 974 F.3d at 188 (The Court is "not required to credit conclusory allegations or legal conclusions couched as factual . . . allegations.").

Courts both in this District and elsewhere have rejected allegations of a CFAA conspiracy far less conclusory than those in the Complaint. For example, in *Hyo Jung v. Chorus Music Studio, Inc.*, No. 13 CIV. 1494 (CM) (RLE), 2014 WL 4493795 (S.D.N.Y. Sept. 11, 2014), this Court refused to consider "conclusory allegations" of a counterclaimed CFAA conspiracy, including allegations that "Plaintiff Hong conspired with other named Plaintiffs in the main action to take Chorus' proprietary information for use in a lawsuit against Defendants," "Plaintiffs aided and abetted Plaintiff Hong in the theft of Chorus' electronic proprietary information," and "Plaintiffs sold the subject customer lists to third parties and unjustly enriched themselves." *Id.* at *7. The

Court also held insufficient the allegations that the Plaintiff employees quit on the same day, had previously discussed quitting, and appeared on an advertisement for a new business venture were insufficient to establish a conspiracy to steal defendants' proprietary information for use in their new business venture because those parts of the complaint "merely allege[d] parallel conduct . . ., which is not sufficient to establish conspiracy." *Id.*

Similarly, in *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285 (M.D. Fla. 2012), the court found allegations that "[co-conspirators] had conspired and hijacked Plaintiff's code and trade secret information" and "conspired to steal and used Plaintiffs' trade secrets . . . to help launch a competing company" were insufficient to state a CFAA conspiracy claim because "they allege no factual basis to support th[ese] claim[s]" other than communication between the alleged co-conspirators and involvement in the formation of a competitor company. *Id.* at 1293–94. Absent allegations that the co-conspirators "assisted" in the taking, or "knew of or were informed about [the CFAA violator]' plans and encouraged or induced him" to commit the violation, the CFAA claim could not stand. *Id.* at 1294.

Finally, as noted above, this Court previously rejected one of Plaintiff's prior CFAA claims on the same grounds. *See Buchanan*, 2021 WL 5889341, at *13 (finding that Omari "fail[ed] to plausible allege that Defendants—as opposed to someone else—were responsible for the purported hacking of El Omari's computer or conspired with Alison to do so"). That conclusion holds again here.

Indeed, in the end, Plaintiff's conclusory allegations fall far short of alleging Dechert was informed of and "encouraged or induced" anyone in an unauthorized access scheme. *Trademotion*, 857 F. Supp. 2d at 1294. Given the absence of any factual basis "to bring the claim from the possible to the plausible," the CFAA conspiracy claim should be dismissed. *Id.*

III. Plaintiff's Conversion Claim is Barred by the Statute of Limitations

Plaintiff's conversion claim under North Carolina law fails because it is clearly time barred. Conversion claims are subject to a three-year statute of limitations in North Carolina. *See* N.C. Gen. Stat. § 1–52(4); *see also Honeycutt v. Weaver*, 257 N.C. App. 599, 609 (2018). And North Carolina courts have held that a "discovery rule" does not apply to conversion claims under North Carolina law because N.C. Gen. Stat. § 1–52(4) does not contain language providing for one, as do other subsections of Gen. Stat. § 1–52. *See White v. Consol. Plan., Inc.*, 166 N.C. App. 283, 310 (2004). Thus, a conversion claim "accrues, and the statute of limitations begins to run, when the unauthorized assumption and exercise of ownership occurs—not when the plaintiff discovers the conversion." *Stratton v. Royal Bank of Canada*, 211 N.C. App. 78, 83 (2011).

Plaintiff alleges that Defendants converted his emails on January 12, 2017. Compl. ¶ 69. Because he did not file his Complaint until June 1, 2023—more than six years after the alleged conversion—his conversion claim is time barred. *See Ferro v. Vol Vo Penta of the Americas, LLC*, No. 17 CIV. 194 (BO), 2017 WL 3710071, at *4 (E.D.N.C. Aug. 28, 2017), *aff'd sub nom. Ferro v. Volvo Penta of the Americas, LLC*, 731 F. App'x 208 (4th Cir. 2018) (applying North Carolina law and concluding conversion claim time barred when "conversion occurred more than three years before the filing of [plaintiff's] complaint").

CONCLUSION

For the foregoing reasons, Dechert respectfully requests that the Court dismiss Plaintiff's Complaint.

Dated: August 25, 2023
New York, New York

By: _____

Sean Hecker
John C. Quinn
David Gopstein
Mark Weiner
KAPLAN HECKER & FINK LLP
350 Fifth Avenue, 63rd Floor
New York, NY 10118
Tel: (212) 763-0883
Fax: (212) 564-0883
shecker@kaplanhecker.com
jquinn@kaplanhecker.com
dgopstein@kaplanhecker.com
mweiner@kaplanhecker.com

Carmen Iguina González*
KAPLAN HECKER & FINK LLP
1050 K Street NW, Suite 1040
Washington, DC 20001
Tel: (212) 763-0883
Fax: (212) 564-0883
ciguinagonzalez@kaplanhecker.com

Attorneys for Defendant Dechert LLP

**Pro Hac Vice Application Forthcoming*